The Honorable Robert S. Lasnik

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. PAIGE A. THOMPSON, Defendant.	NO. CR19-159-RSL GOVERNMENT'S FILING CONCERNING DEFENDANT'S PROPOSED JURY INSTRUCTIONS

The United States of America, by and through Nicholas W. Brown, United States Attorney for the Western District of Washington, and Andrew C. Friedman, Jessica M. Manca, and Tania M. Culbertson, Assistant United States Attorneys for said District, hereby submits this filing concerning Defendant's Proposed Jury Instructions. This filing does not address all of Defendant's proposed instructions, but does address several that present the most substantial concern.

A. Defendant's Requested Instruction No. 7

Thompson has proposed a version of the instruction for wire fraud that adds the following language to the pattern instruction:

> The government must show that some actual harm or injury was contemplated to the victim's property by the defendant. In making that determination the harm or injury

> contemplated must be towards Capital One, Michigan State University, Ohio Department of Public Safety, Digital Ai (formerly Arxan Technologies, Inc.), Enghouse Interactive, Inc., Bitglass, or 42 Lines, Inc. Amazon Web Services is not a victim.

Defendant's Requested Instr. No. 7 (Dkt. No. 286).

This first sentence of this proposed addition appears to be based upon *United States v. Miller*, 953 F.3d 1095, 1102 (9th Cir. 2020), since Thompson cites that as support for her proposed instruction, and since it essentially quotes directly from that opinion. As recognized in the Comment to Model Instruction 15.35, *Miller* held that the then-pattern instruction, the third element of which required the government to prove that a defendant acted with the intent "to deceive or cheat," was incorrect, and that the wire fraud statute required an intent "to deceive and cheat." Ninth Cir. Mod. Jury Instr. 15.35, Comment. As a result, the pattern instruction was amended and the third element now requires intent "to deceive and cheat." Ninth Cir. Mod. Jury Instr. 15.35 (Rev. Jun 2021). The court should not alter the balance of the instruction – approved by the Ninth Circuit Jury Instruction Committee - by adding the additional language that the defendant requests.

The second sentence of the proposed addition appears to be designed to be based upon *United States v. Lew*, 875 F.2d 219, 221-22 (9th Cir. 1989), which Thompson also cites as support for her proposed instruction. That case held that the wire fraud statute required that a defendant intended to obtain property from the party the defendant deceived (as opposed to some third party). The Court should not include the second sentence in its instruction for two reasons. First, *Lew* has been accepted law for more than three decades, yet language of the sort that Thompson seeks has neither been added to the pattern instruction, nor is it generally given, because the language is unnecessary. The Court should not alter the balance of the pattern instruction by including such language.

Second, Thompson's proposed instruction incorrectly reflects the charge. Thompson's instruction would limit the entities the government could prove were defrauded to Capital One and six numbered victims identified in the wire fraud count. But Count 1 of the Second Superseding Indictment alleges that Thompson defrauded "more than 30 different entities, including Capital One, [and seven numbered victims]" from whom she stole data. *See* Second Superseding Indictment ¶ 20 (Dkt. No. 166). It also alleges that she defrauded an unspecified number of victims from whom she stole computing power to mine cryptocurrency. *See id.* ¶ 21. As a result, the Court should not arbitrarily narrow the government's case by including the language that Thompson seeks in its instruction.

B. Defendant's Requested Instruction Nos. 8-10

Count 1 of the Second Superseding Indictment charges Thompson with a fraud scheme with two objects - one of them to steal data from more than 30 different entities. *See* Second Superseding Indictment ¶ 20. Thompson has requested three instructions that would require the government to prove that the data meets the definition of a trade secret under Washington State law in order to be considered property, and that then define various terms in the definition of a trade secret. *See* Defendant's Requested Instr. Nos. 8-10. The Court already has rejected the substance of Thompson's argument, and it should do so again here.

Thompson originally argued in her Motion to Dismiss Counts 1, 9, and 10 (Dkt. No. 158 at 4-5), that the government was required, in order to demonstrate that the data she stole constituted property, to show that it was a trade secret. Thompson relied upon many of the same cases that she now cites as support for her proposed instructions. *See id.* The Court rejected Thompson's argument, noting that "a straightforward application of *Carpenter* . . . compels the conclusion that if the data allegedly copied from Capital One is 'confidential business information,' it is property under the wire fraud statute." Order Denying Motion to Dismiss Counts 1, 9, and 10 (Dkt. No. 202 at 8).

The Court was correct to reject Thompson's argument when she originally made it. As a result, and for the same reasons, it should not give the instructions Thompson now seeks requiring the government to show that the data meets the definition of a trade secret.

C. Defendant's Requested Instruction No. 15

Thompson has proposed an instruction, supposedly based on *Van Buren v. United States*, 141 S. Ct. 1648 (2021), and *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180 (9th Cir. 2022), that

> A person does something "without authorization" when the network is password-protected or is otherwise not publicly accessible, but the person accesses or uses the computer or network anyway.

Defendant's Requested Instr. No. 15. The instruction that Thompson seeks does not accurately reflect the decisions in *Van Buren* or *hiQ*. As a result, the Court should not give this instruction.

The Computer Fraud and Abuse Act (CFAA) imposes criminal liability on any person who "intentionally accesses a computer without authorization or exceeds authorized access," and thereby obtains computer information. 18 U.S.C. § 1030(a)(2). The statute does not define the term "without authorization." It does define the term "exceeds authorized access" to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or to alter." 18 U.S.C. § 1030(e)(6).

Unlike Paige Thompson, who is being prosecuted for accessing a computer without authorization, *Van Buren* involved a prosecution under the exceeding-authorized-access prong of Section 1030. Van Buren, a police officer, accepted $5,000 from a law-enforcement informant to run a license-plate search using a law enforcement database. Van Buren regularly used the database, using valid credentials, as part of his regular duties. But Van Buren's access of the database for money "plainly flouted his department's policy, which authorized him to obtain database information only for law enforcement purposes." *Van Buren*, 141 S. Ct. at 1652. The Supreme Court held that the exceeding-authorized-access prong of Section 1030

> covers those who obtain information from particular areas in the computer—such as files, folders, or databases—to which their computer access does not extend. It does not cover those who, like Van Buren, have improper motives for obtaining information that is otherwise available to them.

Id.

Unlike *Van Buren*, *hiQ* did involve the without-authorization prong of Section 1030, but it involved information that was intentionally made publicly available. LinkedIn, a professional networking site, offered users the opportunity to make their profiles available for viewing by anyone with a web browser. HiQ, a data analytics company, scraped (that is, gathered) that information and used it for business purposes. After LinkedIn sent hiQ a cease-and-desist letter threatening suit under the CFAA, hiQ filed suit seeking a declaratory judgment that the CFAA did not apply.

The Ninth Circuit began its analysis by noting that

> "without authorization" . . . suggests a baseline in which access is not generally available and so permission is ordinarily required. "Authorization" is an affirmative notion, indicating that access is restricted to those specially recognized or admitted. *See, e.g.*, Black's Law Dictionary (11th ed. 2019) (defining "authorization" as "official permission to do something; sanction or warrant").

hiQ, 31 F.4th at 1195-96. The court also noted that "[t]he legislative history of section 1030 thus makes clear that the prohibition on unauthorized access is properly understood to apply to private information – information delineated as private through use of a permission requirement of some sort." *Id.* at 1197. As this Court noted in its order denying Thompson's motion for reconsideration in light of *hiQ*, "the [Ninth Circuit] explained that a 'selective denial of access' is more appropriately characterized as a 'ban' than as a 'lack of "authorization."'" Order at 5 (Dkt. 271) (quoting *hiQ*, 31 F.4th at 1196).

The *hiQ* court ultimately held that hiQ had raised a serious question (the relevant inquiry at the preliminary-injunction stage) as to "whether the reference to access 'without authorization' limits the scope of the statutory coverage to computers for which authorization or access permission, such as password authentication, is generally required." *Id.* The court found that there were three types of computers:

> (1) Computers for which access is open to the general public and permission is not required, (2) computers for which authorization is required and has been given, and (3) computers for which authorization is required but has not been given.

Id. at 1197-98. And it found that, for the first of these groups, the concept of "without authorization" was simply inapt. *Id.* at 1198-99.

The instruction that Thompson proposes does not accurately reflect *Van Buren* and *hiQ*. First, neither *Van Buren* nor *hiQ* suggest the instruction. *Van Buren* did nothing to define authorization, beyond holding that violation of a policy against personal use of a computer that a person *was* authorized to use for official purposes could not constitute unauthorized access. And *hiQ* held only that the concept of authorization did not apply to information that was deliberately and intentionally made publicly accessible.

Second, the reference to "password-protected" networks in the first phrase of the instruction is overly narrow. Passwords are only one form of credentials. Computers may be protected by numerous other forms of credentials, including tokens, access or session keys, and secret access keys. (Notably, the credentials that Thompson stole are access or session keys, secret access keys, and tokens.) Computers also may be protected by other means, such as firewalls. Focusing the instruction on passwords improperly misdirects the jury's inquiry from the actual facts of this case.

Third, and most fundamentally, the standard that the instruction provides—namely that a person acts "without authorization" when a network is "not publicly accessible, but the person accesses or uses the computer or network anyway"—substitutes the concept of public accessibility for the concept of authorization. Nothing in *Van Buren* or *hiQ* suggests this is the law. In fact, the instruction is directly at odds with the reasoning of *hiQ* that authorization is "an affirmative notion" and implies "official permission." 31 F.4th at 1195-96.

The instruction that Thompson proposes would allow anyone who hacked into a computer to argue that the computer was "publicly accessible," by definition, because the hacker was able to access it, and that the hacker therefore had not acted without authorization. The instruction is not the law, it does not reflect the law, and the Court should not give the instruction to the jury.

Dated: June 5, 2022

Respectfully submitted,

NICHOLAS W. BROWN
United States Attorney

s/ Andrew C. Friedman
s/ Jessica M. Manca
s/ Tania M. Culbertson
ANDREW C. FRIEDMAN
JESSICA M. MANCA
TANIA M. CULBERTSON
Assistant United States Attorneys
700 Stewart Street, Suite 5220
Seattle, WA 98101
Phone: (206) 553-7970
Fax: (206) 553-0882
Email: andrew.friedman@usdoj.gov
jessica.manca@usdoj.gov
tania.culbertson@usdoj.gov